DOCKET NO.: 265501US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hisato SHIMA, et al.
SERIAL NO.: NEW U.S. PCT APPLICATION
FILED: HEREWITH
INTERNATIONAL APPLICATION NO.: PCT/JP04/11475
INTERNATIONAL FILING DATE: August 10, 2004
FOR: COMMUNICATION PROCESSING APPARATUS, COMMUNICATION CONTROLLING METHOD AND COMPUTER PROGRAM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2003-291971	12 August 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/11475. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

PCT/JP2004/011475

日本国特許庁
JAPAN PATENT OFFICE

11.08.2004

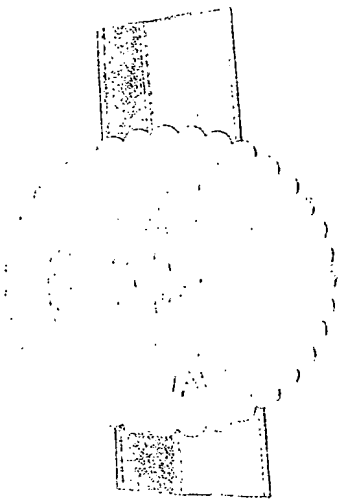
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月１２日

出願番号
Application Number: 特願２００３－２９１９７１

[ST. 10/C]: [ＪＰ２００３－２９１９７１]

出願人
Applicant(s): ソニー株式会社



２００４年　９月１６日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０８３６８０

【書類名】　特許願
【整理番号】　0390562803
【提出日】　平成15年 8月12日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　嶋　久登
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　中野　雄彦
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100093241
　【弁理士】
　【氏名又は名称】　宮田　正昭
　【電話番号】　03-5541-7577
【選任した代理人】
　【識別番号】　100101801
　【弁理士】
　【氏名又は名称】　山田　英治
　【電話番号】　03-5541-7577
【選任した代理人】
　【識別番号】　100086531
　【弁理士】
　【氏名又は名称】　澤田　俊夫
　【電話番号】　03-5541-7577
【手数料の表示】
　【予納台帳番号】　048747
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9904833

【書類名】特許請求の範囲
【請求項１】
ネットワークを介した通信処理を実行する通信処理装置であり、
通信先デバイスの識別情報を異なるデータ処理レベルで複数取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する構成を有することを特徴とする通信処理装置。
【請求項２】
通信先デバイスから受信する少なくとも１つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する構成であることを特徴とする請求項１に記載の通信処理装置。
【請求項３】
前記通信処理装置は、
通信先デバイスから受信する識別情報として、ＯＳＩ参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする請求項１に記載の通信処理装置。
【請求項４】
通信先デバイスから受信する識別情報は、ＩＥＥＥ１３９４規格によって規定されたノードユニークＩＤであることを特徴とする請求項１に記載の通信処理装置。
【請求項５】
前記通信処理装置は、
通信先デバイスから受信する識別情報として、通信先デバイスのＰＨＹ通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする請求項１に記載の通信処理装置。
【請求項６】
通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする請求項１に記載の通信処理装置。
【請求項７】
前記通信処理装置は、
通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、これらの複数のブルートゥースデバイス・アドレスの照合を行う構成であることを特徴とする請求項１に記載の通信処理装置。
【請求項８】
ネットワークを介した通信処理を実行する通信制御方法であり、
通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、
取得した複数の識別情報の照合を実行する照合処理ステップと、
照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、
を有することを特徴とする通信制御方法。
【請求項９】
前記識別情報取得ステップにおいて通信先デバイスから受信する少なくとも１つの識別

情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信することを特徴とする請求項８に記載の通信制御方法。

【請求項１０】

前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、ＯＳＩ参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項８に記載の通信制御方法。

【請求項１１】

通信先デバイスから受信する識別情報は、ＩＥＥＥ１３９４規格によって規定されたノードユニークＩＤであることを特徴とする請求項８に記載の通信制御方法。

【請求項１２】

前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスのＰＨＹ通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項８に記載の通信制御方法。

【請求項１３】

通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする請求項８に記載の通信制御方法。

【請求項１４】

前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする請求項８に記載の通信制御方法。

【請求項１５】

ネットワークを介した通信処理を実行するコンピュータ・プログラムであり、

通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、

取得した複数の識別情報の照合を実行する照合処理ステップと、

照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とするコンピュータ・プログラム。

【書類名】明細書
【発明の名称】通信処理装置、および通信制御方法、並びにコンピュータ・プログラム
【技術分野】
【０００１】
本発明は、通信処理装置、および通信制御方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、例えばホームネットワーク等のローカルネットワーク内に接続された機器と、インターネット等の外部ネットワークに接続されけた機器とを区別可能とした認証を実行して通信を行うことにより、例えばホームネットワーク内でのみ利用の許容されたコンテンツの外部流出など、コンテンツ不正利用処理などを排除可能とした通信処理装置、および通信制御方法、並びにコンピュータ・プログラムに関する。
【背景技術】
【０００２】
昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。
【０００３】
しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。
【０００４】
このようなホームネットワーク内のサーバに格納されたコンテンツや秘密情報は、例えば、インターネットを介した外部からのアクセスによって不正に取得される可能性がある。このような不正アクセスを許容すると、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題である。
【０００５】
このように、映画や音楽など著作権の管理が必要なコンテンツをネットワークを通じて伝送する場合、そのコンテンツ伝送範囲は利用が許可された範囲、例えばホームネットワーク内のデバイス間に留めることが求められるが、近年のインターネットの普及に伴い、インターネットを介したコンテンツの不正な伝送が行われ、問題になっている。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明は、このような状況に鑑みてなされたものであり、ホームネットワーク等の特定のローカルネットワーク内の機器と、インターネット等の外部ネットワークに接続された機器とを明確に区別する認証構成を実現したものである。コンテンツ等のデータ転送の際には、認証処理を実行し、ホームネットワーク等のローカルネットワークの接続機器であることの確認を行う構成とすることで、コンテンツの不正流出、秘密情報の漏洩等の防止を可能とした通信処理装置、および通信制御方法、並びにコンピュータ・プログラムを提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明の第１の側面は、
ネットワークを介した通信処理を実行する通信処理装置であり、
通信先デバイスの識別情報を異なるデータ処理レベルで複数取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する構成を有することを特徴とする通

信処理装置にある。

【０００８】

さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する少なくとも１つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する構成であることを特徴とする。

【０００９】

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、ＯＳＩ参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする。

【００１０】

さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する識別情報は、ＩＥＥＥ１３９４規格によって規定されたノードユニークＩＤであることを特徴とする。

【００１１】

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、通信先デバイスのＰＨＹ通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信し、これらの複数の識別情報の照合を行う構成であることを特徴とする。

【００１２】

さらに、本発明の通信処理装置の一実施態様において、通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする。

【００１３】

さらに、本発明の通信処理装置の一実施態様において、前記通信処理装置は、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、これらの複数のブルートゥースデバイス・アドレスの照合を行う構成であることを特徴とする。

【００１４】

さらに、本発明の第２の側面は、

ネットワークを介した通信処理を実行する通信制御方法であり、

通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、

取得した複数の識別情報の照合を実行する照合処理ステップと、

照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とする通信制御方法にある。

【００１５】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップにおいて通信先デバイスから受信する少なくとも１つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信することを特徴とする。

【００１６】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、ＯＳＩ参照モデルにおける物理層またはデ

ータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

【００１７】

さらに、本発明の通信制御方法の一実施態様において、通信先デバイスから受信する識別情報は、ＩＥＥＥ１３９４規格によって規定されたノードユニークＩＤであることを特徴とする。

【００１８】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスのＰＨＹ通信部の取得した識別情報と、通信先デバイスのネットワーク通信部の取得した識別情報とを受信するステップであり、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

【００１９】

さらに、本発明の通信制御方法の一実施態様において、通信先デバイスから受信する識別情報は、ブルートゥース通信規格によって規定されたブルートゥースデバイス・アドレスであることを特徴とする。

【００２０】

さらに、本発明の通信制御方法の一実施態様において、前記識別情報取得ステップは、通信先デバイスから受信する識別情報として、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づくデータを受信し、前記照合処理ステップは、これらの複数の識別情報の照合を行うことを特徴とする。

【００２１】

さらに、本発明の第３の側面は、

ネットワークを介した通信処理を実行するコンピュータ・プログラムであり、

通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する識別情報取得ステップと、

取得した複数の識別情報の照合を実行する照合処理ステップと、

照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する判定ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００２２】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００２３】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【発明の効果】

【００２４】

本発明の構成によれば、ホームネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部

機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、本発明の判定を伴う認証を実行することによりローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となる。

【００２５】

本発明の構成では、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する。例えば少なくとも１つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成処理によって生成した処理データとして受信する。また、ＯＳＩ参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの複数の識別情報の照合を行う。このように、複数の異なるデータ処理レベルで取得された識別情報の照合を行い、照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かが確実に判定され、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの外部に対する漏洩、流出を未然に防止することが可能となる。

【００２６】

本発明の構成によれば、ＩＥＥＥ１３９４規格におけるノードユニークＩＤや、ブルートゥース規格におけるブルートゥースデバイス・アドレスを適用した比較照合が可能であり、既存の通信において設定済みの識別情報を利用可能となる。

【発明を実施するための最良の形態】

【００２７】

以下、図面を参照しながら本発明の通信処理装置、および通信制御方法、並びにコンピュータ・プログラムの詳細について説明する。

【００２８】

まず、図１を参照して、本発明の適用可能なネットワーク構成例について説明する。図１は、例えば特定ユーザの家等に構築されたホームネットワーク１００等のローカルエリアネットワーク、すなわち内部ネットワークであり、パーソナルコンピュータ（ＰＣ）１０１、１０２、ＴＶ１０３、ハードディスクレコーダ１０４、ＰＤＡ１０５等の様々な情報処理装置がホームネットワーク１００を介してデータ送受信を行う。

【００２９】

たとえば、ＰＣ１０１、１０２、あるいはハードディスクレコーダ１０４をコンテンツ提供サーバとし、ＴＶ１０３、ＰＤＡ１０５をクライアントとして、クライアントがサーバの格納コンテンツをネットワークを介して取得し、クライアントのディスプレイ、スピーカを利用してコンテンツ出力を行う。

【００３０】

ホームネットワーク１００は、有線、無線等いずれかのネットワークであり、各接続機器は、通信パケットをネットワークを介して送受信する。

【００３１】

図１において、ホームネットワーク１００は、インターネット等の外部ネットワーク１２０に接続されている。外部ネットワーク１２０にもＰＣ１２１、携帯電話１２２、ポータブル再生プレーヤ１２３等の各種の通信処理装置が接続される。ホームネットワーク１００内の通信処理装置と外部ネットワーク１２０の通信処理装置とは、外部ネットワーク１２０およびホームネットワーク１００を介して通信が可能となる。

【００３２】

外部ネットワーク１２０およびホームネットワーク１００によって構成される内部ネットワークの間には、外部ネットワーク１２０と内部ネットワーク間の通信を可能とするデータ処理、例えばホームネットワーク内のデータ通信パケットであるＩＥＥＥ１３９４パケットと、外部ネットワークでの転送パケットであるイーサネットパケット、ＩＰパケットの変換などを実行する通信サーバ１１０が接続される。

【００３３】
外部ネットワーク１２０に接続されたＰＣ１２１、携帯電話１２２、ポータブル再生プレーヤ１２３等の各種の通信処理装置は、通信サーバ１１０を介してホームネットワーク１００内のサーバ、例えばＰＣ１０１、１０２、ハードディスクレコーダ１０３等にアクセスし、これらの装置に格納されたコンテンツを取得してＰＣ１２１、携帯端末１２２、再生プレーヤ１２３等においてコンテンツ出力を行うことが可能となる。
【００３４】
ただし、これらのコンテンツ取得を不特定のクライアントに許容することは、コンテンツの著作権、秘密漏洩等の問題から好ましいことではない。従って、機器間の通信においては、後段で説明する本発明の認証シーケンスに従った認証処理を実行し、内部ネットワーク内のデータが外部に不正に流出するのを防止する構成としている。この詳細処理構成については後述する。
【００３５】
図１に示す各ルットワーク接続機器としての通信処理装置のハードウェア構成例について図２を参照して説明する。
【００３６】
ＣＰＵ(Central Processing Unit)２０１は、ＲＯＭ(Read Only Memory)２０２、またはＨＤＤ(Hard Disk Drive)２０４等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。ＲＡＭ(Random Access Memory)２０３には、ＣＰＵ２０１が実行するプログラムやデータが適宜記憶される。ＣＰＵ２０１、ＲＯＭ２０２、およびＲＡＭ２０３、ＨＤＤ２０４は、バス２０５を介して相互に接続されている。
【００３７】
バス２０５には、入出力インタフェース２０６が接続されており、この入出力インタフェース２０６には、例えば、ユーザにより操作されるキーボード、スイッチ、ボタン、あるいはマウス等により構成される入力部２０７、ユーザに各種の情報を提示するＬＣＤ、ＣＲＴ、スピーカ等により構成される出力部２０８が接続される。さらに、データ送受信手段として機能する通信部２０９、さらに、磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体２１１を装着可能で、これらのリムーバブル記録媒体２１１からのデータ読み出しあるいは書き込み処理を実行するドライブ２１０が接続される。通信部２０９は、例えばＩＥＥＥ１３９４規格に従った通信、あるいはブルートゥース規格に従った通信処理の可能な構成を持つ。
【００３８】
なお、図２に示す構成は、図１に示すネットワーク接続機器の一例としての一般的なＰＣの構成を示すものであるが、ネットワーク接続機器はＰＣに限らず、図１に示すように携帯電話、ＰＤＡ等の携帯通信端末、その他の様々な電子機器、通信処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。
【００３９】
本発明の通信処理装置において実行する機器間の通信においては、まず機器間の認証処理を実行し、認証処理の結果、通信相手が同一のホームネットワーク等のローカルネットワーク接続された機器であることが確認された場合に、コンテンツ等のデータ転送を許容する。認証処理においては、通信先デバイスの識別情報を異なるデータ処理レベルで複数取得し、取得した複数の識別情報の照合を行い、該照合の成立または非成立に基づいて、通信先デバイスが通信元である自デバイスの接続されたローカルネットワークと同一のローカルネットワークに接続されたデバイスであるか否かを判定する処理を実行する。
【００４０】
１つの具体例としては、例えば通信機器の識別子（ＩＤ）をＯＳＩ参照モデルにおける物理層やデータリンク層での通信と、ネットワーク層以上の例えばアプリケーション層での通信においてそれぞれ受領し、この２つのＩＤを比較する処理を行う。以下、本発明に

従った認証処理の具体例について、ＩＥＥＥ１３９４規格に従った通信を行う構成例と、ブルートゥース規格に従った通信を行う構成例について説明する。

【００４１】

（１）ＩＥＥＥ１３９４規格に従った通信を行う構成例

ホームネットワーク等のローカルネットワークに接続された通信処理装置は、ＩＥＥＥ１３９４データインターフェイスを備え、ＩＥＥＥ１３９４方式に従ったデータ転送を実行する。ＩＥＥＥ１３９４データインターフェイスは、例えばＳＣＳＩなどよりもデータ転送レートが高速であり、所要のデータサイズを周期的に送受信することが保証されるアイソクロナス（Ｉｓｏｃｈｒｏｎｏｕｓ）通信が可能である。このため、ＩＥＥＥ１３９４データインターフェイスは、ＡＶ(Audio/Video)などのストリームデータをリアルタイムで転送するのに有利となる。

【００４２】

ＩＥＥＥ１３９４によるデータ伝送方式には、上述のアイソクロナス（Ｉｓｏｃｈｒｏｎｏｕｓ）通信方式と、非同期で通信するアシンクロナス（Ａｓｙｎｃｈｒｏｎｏｕｓ）通信方式が存在する。一般に、アイソクロナス（Ｉｓｏｃｈｒｏｎｏｕｓ）通信方式はデータの送受信に用いられ、アシンクロナス（Ａｓｙｎｃｈｒｏｎｏｕｓ）通信方式は各種制御コマンドの送受信に用いられる。１本のケーブルを使用して、これら２種類の通信方式によって送受信を行うことができる。

【００４３】

各種デジタルＡＶ機器やパーソナルコンピュータ装置等の電子機器を、ＩＥＥＥ(Institute of Electrical Engineers)１３９４等のデジタルデータインターフェイス規格に従ったデータバスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システムが構築される。

【００４４】

このようなＡＶシステムでは、いわゆるリモート制御も可能となる。例えば、データバスを介してディスク記録再生装置とパーソナルコンピュータが接続されると、ディスク記録再生装置に対する記録再生、更には記録ソースの編集などに関する操作をパーソナルコンピュータ装置側での操作によって行うことも可能となる。

【００４５】

本発明の通信処理装置としてのＩＥＥＥ１３９４対応機器の構成について図３を用いて説明する。

【００４６】

送受信部３０１の内部には、データ処理手段としてＰＨＹ－ＩＣ３０３、ＬＩＮＫ－ＩＣ３０４、ネットワーク通信部（ＩＥＥＥ１３９４制御マイコン）３０５を有する。なお、ＰＨＹ－ＩＣ３０３とＬＩＮＫ－ＩＣ３０４をまとめてＰＨＹ通信部とみなす。

【００４７】

ＰＨＹ－ＩＣ３０３は、物理層の電気的インタフェースを受け持ち、ＬＩＮＫ－ＩＣ３０４からのパラレルデータをシリアル変換し、ＩＥＥＥ１３９４規格の電気信号を発生し、逆にＩＥＥＥ１３９４規格信号をシリアルデータに戻しパラレルデータとしてＬＩＮＫ－ＩＣ３０４に送信する。また、ＰＨＹ－ＩＣ３０３は、バス（ケーブル）の状態認識、バスの初期化、アービトレーション処理などを実行する。すなわち、ＰＨＹ－ＩＣ３０３は、ＩＥＥＥ１３９４規格のプロトコルに従って、ＩＥＥＥ１３９４端子３０２を介してＩＥＥＥシリアルバス３１０との間の通信を制御し、ＩＥＥＥ１３９４シリアルバス３１０から供給されるデジタルビデオデータやデジタルオーディオデータがパケット化されたアイソクロナスパケット、または制御信号がパケット化されたアシンクロナスパケットをＬＩＮＫ－ＩＣ３０４に供給する。ＰＨＹ－ＩＣ３０３はまた、ＬＩＮＫ－ＩＣ３０４から供給されるアイソクロナスパケットやアシンクロナスパケットを、ＩＥＥＥ１３９４シリアルバス３１０に出力する。

【００４８】

ＬＩＮＫ－ＩＣ３０４は、データリンク層を受け持ち、送信データパケットのＰＨＹ－

ＩＣ３０３への送出、ＰＨＹ－ＩＣ３０３受信パケットのトランザクション／アプリケーション層への送出を実行する。すなわち、ＰＨＹ－ＩＣ３０３から供給されるアシンクロナスパケットを、ＩＥＥＥ１３９４制御マイコン３０５が解読できるデジタル信号（コマンド）に変換し、ＩＥＥＥ１３９４制御マイコン３０５に供給したり、ＩＥＥＥ１３９４制御マイコン３０５から供給されるデジタル信号をアシンクロナスパケットに変換し、ＰＨＹ－ＩＣ３０３に供給する。ＬＩＮＫ－ＩＣ３０４はまた、ＰＨＹ－ＩＣ３０３から供給されるアイソクロナスパケットをデジタル信号に変換したり、機器から入力される主データ（例えば、デジタルビデオデータ、デジタルオーディオデータ）を、アイソクロナスパケットに変換し、ＰＨＹ－ＩＣ３０３に供給する。

【００４９】

ネットワーク通信部（ＩＥＥＥ１３９４制御マイコン）３０５は、ＬＩＮＫ－ＩＣ３０４から供給されたコマンドを機器制御マイコン３０６に転送するとともに、そのコマンドに対応するレスポンスを生成し、ＬＩＮＫ－ＩＣ３０４に出力する。

【００５０】

機器制御マイコン３０６は、ネットワーク通信部（ＩＥＥＥ１３９４制御マイコン）３０５から供給されたコマンドに対応して、機器内部の回路（図示せず）を制御し、各種の処理を実行させる。

【００５１】

ＬＩＮＫ－ＩＣ３０４は、ＥＰＲＯＭなどのメモリ３２１が接続ないし内蔵され、メモリ３２１に書き込まれたＩＤを読み取ることができる。図では、メモリ３２１をＬＩＮＫ－ＩＣ３０４に内蔵した例を示している。

【００５２】

メモリ３２１に格納されるＩＤは、グローバルユニーク（Global Unique）な値を用いるものとする。また、ＬＩＮＫ－ＩＣ３０４、メモリ３２１は、耐タンパ構成を持つパッケージとして構成され、ＩＤや通信内容の改ざんの困難性を高めた構成を持つ。ＩＤの改ざんを困難にする方法の具体例としては、例えば、ＬＩＮＫ－ＩＣ３０４とＩＤの格納メモリ３２１を１つのＩＣで構成することや、複数のＩＣで構成される場合はＩＣ間の通信を保護するために通信路を暗号化したり、あるいはＩＣをＢＧＡパッケージにして、配線を基板の内層に埋め込んで信号にアクセスできなくするといった構成とするなどの各種構成が適用可能である。

【００５３】

ネットワーク通信部（ＩＥＥＥ１３９４制御マイコン）３０５は、ＬＩＮＫ－ＩＣ３０４を通じて他のネットワーク接続機器のネットワーク通信部と通信を行うことができる。また、各ネットワーク通信部は、自身のＬＩＮＫ－ＩＣ３０４経由でＩＤを読み取ることができる。

【００５４】

以上のように構成される１３９４対応機器は、ＩＥＥＥ１３９４シリアルバス３１０を介して、他の各接続機器とデータ送受信、通信を実行することができる。

【００５５】

例えばＩＥＥＥ１３９４対応機器としてのＶＴＲに所定の機能を実行させるとき、ＩＥＥＥ１３９４バスに接続されたパーソナルコンピュータ（ＰＣ）は、その機能の実行を指令する、例えば、再生、記録、巻戻しなどのＡＶ／Ｃコマンド（以下、これらをまとめてＡＶ／Ｃコマンドと称する）を、ＩＥＥＥ１３９４シリアルバスを介してＶＴＲに伝送する。

【００５６】

ＶＴＲは、ＡＶ／Ｃコマンドを受信すると、それに対応した処理を実行するとともに、所定のレスポンスをＡＶ／Ｃコマンドの送信元である、パーソナルコンピュータ（ＰＣ）に出力する。

【００５７】

図４を参照して、ネットワーク接続機器間の通信の際に実行する認証処理シーケンスに

ついて説明する。

【００５８】

図４に示すフローは機器Ａが、通信を行おうとする機器Ｂが適切な通信相手であるかを確認し、通信の可否を制御するフローである。すなわち、機器Ａは、機器Ｂが機器Ａと同一のホームネットワーク内の内部ネットワーク接続機器であるか、インターネット等の外部ネットワークに接続された機器であるかを判別する。

【００５９】

まず、機器Ａは、ステップＳ１１１において、相手機器ＢのＰＨＹ通信部に対するコマンドとして、ＩＤ要求コマンド１を送る。機器ＢのＰＨＹ通信部は、ステップＳ１１２において、ＩＤ要求を受けると、ステップＳ１１３において、ＰＨＹ通信部の処理として自身のＩＤを読み出して、ステップＳ１１４において、機器Ａに対して返送する。

【００６０】

機器Ａは、ステップＳ１１５において、機器ＢのＰＨＹ通信部からのＩＤを受信し、受信ＩＤを、後の処理のために記憶しておく。以上の通信は、ＯＳＩ参照モデルのデータリンク層以下で実施されるものとし、ブリッジやルーターを介さないネットワーク接続機器間の通信においてのみ可能なものとする。

【００６１】

次に機器Ａは、ステップＳ１１６において、機器Ｂのネットワーク通信部に対するコマンドとして、ＩＤ要求コマンド２を送る。機器Ｂのネットワーク通信部は、ステップＳ１１７において、ＩＤ要求コマンド２を受けると、機器Ｂのネットワーク通信部は、ステップＳ１１８において、自身のＰＨＹ通信部経由でメモリに格納されたＩＤを読み出して、ステップＳ１１９において機器Ａに対して読み出したＩＤを返送する。この通信は、ＯＳＩ参照モデルのネットワーク層以上で実施されるものとし、ブリッジやルーターを介した機器とも通信可能なものとする。なお、この通信で得たＩＤを以後、ＩＤ'とする。

【００６２】

機器Ａは、ステップＳ１２０において、機器Ｂのネットワーク通信部からＩＤ'を受信すると、ステップＳ１２１において、受信したＩＤ'が、先に機器ＢのＰＨＹ通信部から受信したＩＤと一致するか確認する。

【００６３】

一致した場合、すなわちＩＤ＝ＩＤ'が成立する場合は、ステップＳ１２２に進み、相手機器との通信を許可し、引き続く通信を行う。一方、一致しない場合、すなわちＩＤ＝ＩＤ'が成立しない場合は、ステップＳ１２３に進み、以後の通信を禁止する。

【００６４】

機器間の通信は、通信途上での改ざんやなりすましを防止するため、両方の機器が共有する秘密データに基づいて保護された状態で行われることも考えられる。例えば暗号化したり、通信内容に対する電子署名や鍵付きハッシュ値を送るなどの手段が適用されうる。

【００６５】

図５に、ネットワーク通信部からのＩＤ送信の際に、特定の正当な機器のみが保持する秘密情報としての鍵を適用した暗号処理やハッシュ値生成処理によって取得ＩＤのデータ処理を実行し、暗号化データあるいはハッシュ値としてのＩＤを送信する構成とした例について説明する。

【００６６】

機器Ａは、ステップＳ２０１において、相手機器ＢのＰＨＹ通信部に対するコマンドとして、ＩＤ要求コマンド１を送る。機器ＢのＰＨＹ通信部は、ＩＤ要求を受けると、ステップＳ２０２において、ＰＨＹ通信部の処理として自身のＩＤを読み出して、ステップＳ２０３において、機器Ａに対して返送する。

【００６７】

機器Ａは、機器ＢのＰＨＹ通信部からのＩＤを受信し、受信ＩＤを、後の処理のために記憶しておく。次に、ステップＳ２０４において、機器Ｂのネットワーク通信部に対するコマンドとして、ＩＤ要求コマンド２を送る。機器Ｂのネットワーク通信部は、ＩＤ要求

コマンド２を受けると、ステップＳ２０５において、自身のＰＨＹ通信部経由でメモリに格納されたＩＤを読み出して、機器Ａと機器Ｂが共有する秘密データ、すなわち暗号処理鍵やハッシュ値生成鍵を適用し、読み出したＩＤに対する暗号処理鍵を適用した暗号化、あるいはハッシュ値生成鍵を適用したハッシュ値生成処理を行い、生成したデータをステップＳ２０６において、機器Ａに送信する。

【００６８】

機器Ａは、受信したＩＤ２が例えば暗号化データである場合は、機器Ｂと共有する鍵に基づいて復号処理を実行し、復号結果として得られたＩＤ２と先にＰＨＹ通信部から受信したＩＤ１とを照合比較する。両者が一致すれば、ＩＤ１を送信した機器とＩＤ２を送信した機器とは同一であり、ＰＨＹ通信部の通信が実行可能な内部ネットワーク接続機器との通信が実行されていると判定し、その後の通信、例えばコンテンツ提供を行う。ＩＤ１とＩＤ２が一致しない場合は、ＩＤ１を送信した機器とＩＤ２を送信した機器とは同一でない。すなわち、ＩＤ１は、ＰＨＹ通信部の通信が実行可能な内部ネットワーク接続機器が機器Ａに提供し、ＩＤ２はインターネット等、外部ネットワークに接続された機器が機器Ａに送信してきたものと判定し、不正な外部からのアクセスが行われていると判定し、その後の通信、例えばコンテンツ提供を実行することなく、通信を停止する。

【００６９】

また、機器Ａは、受信したＩＤ２が例えばハッシュ値である場合は、先にＰＨＹ通信部から受信したＩＤ１に対して、機器Ｂと共有するハッシュ値生成鍵に基づいてハッシュ値を生成し、結果として得られたＩＤ１に基づくハッシュ値と、機器Ｂのネットワーク通信部から受信したＩＤ２に基づくハッシュ値とを照合比較する。両者が一致すれば、ＩＤ１を送信した機器とＩＤ２を送信した機器とは同一であり、ＰＨＹ通信部の通信が実行可能な内部ネットワーク接続機器との通信が実行されていると判定し、その後の通信、例えばコンテンツ提供を行う。不一致の場合は、上述と同様、外部からの不正アクセスであると判定し、その後の通信、例えばコンテンツ提供を実行することなく、通信を停止する。

【００７０】

本発明の上述した認証シーケンスを実行することにより、ローカルネットワークに接続された機器と、外部ネットワーク接続機器とを区別することが可能となり、外部ネットワークを介した不正アクセスを排除することができる。

【００７１】

すなわち、図６（ａ）に示すように、ローカルバス上に接続された機器Ａ４１１と機器Ｂ４１２がある場合、機器Ａは、上述した認証シーケンスにおいて機器Ｂから受信するＩＤはＩＤ１＝ＩＤ２となる。しかし、図６（ｂ）に示すように、機器Ａ４２１が外部ネットワークに接続された機器Ｃ４２２と接続して、上述の認証シーケンスを実行した場合、機器Ａ４２１はローカル接続した機器Ｘ４３１のＰＨＹ通信部からＩＤ１を受信し、機器Ｃ４２２のネットワーク通信部からＩＤ２を受信することになる。この場合ＩＤ１＝ＩＤ２は成立せず、機器Ａ４２１は、外部ネットワーク接続機器からのアクセスであると判定し、通信を終了することができる。

【００７２】

なお、上記処理において、機器間で送受信するＩＤは、ＩＥＥＥ１３９４規定において定められているノードユニークＩＤを適用することが可能である。

【００７３】

ＩＥＥＥ１３９４では、コンフィグレーションＲＯＭに６４ビットのノードユニークＩＤを持つことが規定されている。このＩＤは、ＩＥＥＥ１３９４で規定されたアシンクロナス通信によって直接参照することができる。通常ノードユニークＩＤの情報は、ＩＥＥＥ１３９４のＩＣだけで処理が完結する。一方、ＩＥＥＥ１３９４のＩＣを実装する装置において、そのＩＣ以外のＩＣ、例えばＣＰＵからＩＥＥＥ１３９４のＩＣ経由でノードユニークＩＤを読み取ることができれば、上述した直接的な参照方法以外の方法でＩＤを受け渡すこともできる。例えば上述したように２つの機器が共有する秘密鍵を用いた暗号化データとして送受信することができる。

【００７４】
ＩＥＥＥ１３９４の機器同士で、本発明の処理を実行する場合、通信相手を１３９４のローカルバス内の機器に限定するため、１３９４の１０ビットのバスＩＤは全ビット１とし、ブリッジを経由した異なるバス上の機器とは通信を行わないことを前提とする。
【００７５】
しかし、先に説明した図６（ｂ）のように、機器Ｘが機器Ｃに、また機器Ｙが機器Ａになりすますことで、ローカルバスを越えた通信を行うことも可能である。これを防ぐために機器Ａは、通信相手のコンフィグレーションＲＯＭにアノセスし、ノードユニークＩＤを直接参照するとともに、前述の別のプロトコルによってもＩＤを取得する。この場合、機器Ａは、ローカルバス上にいる機器Ｘのコンフィグレーション ＲＯＭを参照することしかできず、機器Ｘのノードユニーク ＩＤを参照する一方、機器Ａと秘密鍵を共有する機器は、機器Ｃなので、機器Ｘ，Ｙ経由で機器ＣのＩＤを取得することになる。これらのＩＤは一致しないことになり、結果として機器Ａは、機器Ｃがローカルバス上に存在しないことを検知し、中継された通信を防止することができる。
【００７６】
（２）ブルートゥース規格に従った通信を行う構成例
次に、ホームネットワーク等のローカルネットワークに接続された通信処理装置が、ブルートゥース規格に従った通信を行う構成例について説明する。
【００７７】
近年、近距離間の無線通信手段としてブルートゥース（Bluetooth）が注目されており、様々な対応機器が開発、販売されている。
【００７８】
このブルートゥースによる無線通信システムは、従来のＩｒＤＡ（Infrared Data Association）のような赤外線通信方式と比較して、指向性がなく、透過性が高いなどの長所を有している。従って、ＩｒＤＡなどの指向性が強い通信を利用する際には、通信を行わせる機器同士を適切に向かい合わせる必要があったが、ブルートゥースなどの通信システムでは、そのような位置の制約は不要となる。
【００７９】
ブルートゥースの規格に関しては、Bluetooth SIG Inc.によって管理されており、その詳細については、Bluetooth SIG Inc.から誰でも入手することが可能であるが、例えば、ブルートゥースを用いた通信においては、通信を制御するマスタと呼ばれる機器から、周囲に存在する機器を検出するための機器検出メッセージがブロードキャスト送信される。
【００８０】
そして、マスタは、この機器検出メッセージを受信した機器（スレーブ）から送信されてきた応答メッセージによって、周囲に存在する機器、すなわち通信可能な機器を検出することができる。
【００８１】
また、マスタは、検出した機器の中から、特定の機器との間で通信を確立する場合、応答メッセージに含まれるそれぞれの機器の識別情報に基づいて機器を特定し、その通信を確立する。
【００８２】
ブルートゥースにおいては、そのような機器を識別する情報としてブルートゥースデバイス・アドレスと呼ばれる情報が個々の機器に付与されており、それぞれの機器に対して固有（一義的）であることから、機器の管理等、様々な処理に利用される。
【００８３】
図７を参照して、ブルートゥース規格に準拠した無線通信ネットワークとしてのピコネットを形成して、ピコネットを形成した通信処理装置間で、相互に各種のデータを送受信する通信システムの構成例について説明する。
【００８４】
前述したように、ブルートゥースを用いた通信においては、通信を制御するマスタと呼

ばれる機器と、マスタを介した通信を実行する複数のスレーブと呼ばれる機器によって形成されるネットワーク（ピコネット）において通信が実行される。ブルートゥースにおいては、各機器を識別する情報としてブルートゥースデバイス・アドレスが個々の機器に設定され、ブルートゥースデバイス・アドレスに基づいて、通信対象の特定がなされる。

【００８５】

マスタとスレーブからなるピコネットにおいては、１つのマスタに対して、最大７つのスレーブが属することができる。同一のピコネットに属する全ての機器は、周波数軸（周波数ホッピングパターン）と時間軸（タイムスロット）が同期している状態にある。

【００８６】

図７においては、パーソナルコンピュータ（ＰＣ）５０１がマスタとして設定され、その他の機器、パーソナルコンピュータ（ＰＣ）５２１、携帯電話５２２、ＰＤＡ（Personal Digital Assistants）５２３、ビデオカメラ５２４が各々スレーブとして設定された構成例を示している。

【００８７】

これらの１つのマスタと複数のスレーブによって構成されるピコネットは、他の外部ネットワークと接続しない独立したネットワーク（アドホックモード）として存在することも、あるいはインターネット、あるいは他のピコネット等、他のネットワークにマスタを介して接続した構成（インフラストラクチャモード）とすることも可能である。

【００８８】

このピコネットは、パーソナルエリアネットワーク（ＰＡＮ）とも呼ばれ、スレーブの各々は、ＰＡＮＵ（ＰＡＮユーザ：PAN User）と呼ばれる。また、他のネットワークと接続された構成（インフラストラクチャモード）におけるマスタは、ピコネットを構成するスレーブ間の通信パケットの中継、すなわちパケット交換処理を実行するとともに、外部接続ネットワークとのパケット交換も実行し、ＮＡＰ（Network Access Point）と呼ばれる。一方、他の外部ネットワークと接続しない独立したネットワーク（アドホックモード）におけるマスタは、ピコネットを構成するスレーブ間の通信パケットの中継を行ない、ＧＮ（Group Ad-hoc Network）と呼ばれる。

【００８９】

ブルートゥースにおいては、無線通信で送受信されるデータや、その通信手順に関して、サービス毎に取り決めたプロファイルと呼ばれる仕様が策定されており、このプロファイルに従って、各機器が提供できるサービスが表わされている。ＰＡＮ(Personal Area Network)プロファイルでは、ピコネットにおけるスレーブ間の通信方法が規定されており、ＰＡＮプロファイルに基づいて構成されたピコネットに属する機器は、そのピコネットを１つのネットワークとして各種のデータを送受信する。

【００９０】

図７に示すマスタとしてのパーソナルコンピュータ（ＰＣ）５０１、スレーブとしてのパーソナルコンピュータ（ＰＣ）５２１、携帯電話５２２、ＰＤＡ５２３、ビデオカメラ５２４は、それぞれブルートゥースモジュールを内蔵しており、ブルートゥース規格に準拠した無線通信により、相互に各種のデータを送受信できるようになされている。

【００９１】

マスタ、スレーブを構成する各機器には、ブルートゥース規格に準拠した無線通信を実行するためのブルートゥースモジュールが備えられる。具体的には、無線周波数として、２．４ＧＨｚのＩＳＭ帯を使用した時分割多重方式を採用し、ＩＳＭ帯において周波数ホッピングスペクトラム拡散通信による無線通信を行なうためのモジュールである。

【００９２】

ブルートゥースモジュールの具体的構成例について、図８を参照して説明する。ＣＰＵ６０１は、ＲＯＭ６０２に格納されている制御プログラムをＲＡＭ６０３に展開し、ブルートゥースモジュール６００の全体の動作を制御する。ＣＰＵ６０１は、データ処理手段、あるいは通信制御処理手段として機能する。これらのＣＰＵ６０１乃至ＲＡＭ６０３は、バス６０５を介して相互に接続されており、このバス６０５には、また、フラッシュメ

モリ６０４が接続されている。

【００９３】

フラッシュメモリ６０４には、例えば、ピコネットを構成するマスタ、スレーブそれぞれのブルートゥースデバイスに設定されているブルートゥースデバイス名、および、それぞれのブルートゥースデバイスに対して固有なブルートゥースデバイス・アドレスなどが記憶されている。

【００９４】

このブルートゥースデバイス・アドレスは、４８ビットの識別子であり、それぞれのブルートゥースデバイスに対して固有（一義的）であることから、ブルートゥースデバイスの管理に関する様々な処理に利用される。

【００９５】

例えば、ピコネット内同期を確立するためには、全てのスレーブがマスタの周波数ホッピングパターンに関する情報を取得している必要があり、この周波数ホッピングパターンは、マスタのブルートゥースデバイス・アドレスに基づいてスレーブにより算出されるようになされている。

【００９６】

より詳細には、ブルートゥースデバイス・アドレスは、図９に示すように、２４ビットのロー・アドレスパート（ＬＡＰ：Low Address Part）と、８ビットのアッパー・アドレスパート（ＵＡＰ：Upper Address Part)と、そして残りの１６ビットのノンーシグニフィカントアドレスパート（ＮＡＰ：Non-significant Address Part)とそれぞれ区分された構成を持ち、周波数ホッピングパターンの算出には、ＬＡＰ全体の２４ビットとＵＡＰの下位４ビットからなる２８ビットが用いられる。

【００９７】

スレーブの各々は、ピコネット内同期を確立するための「呼び出し（Ｐａｇｅ）」により取得したマスタのブルートゥースデバイス・アドレスの、上述した２８ビットの部分と、同様にマスタから通知されたブルートゥースクロックに基づいて、周波数ホッピングパターンを算出することができる。

【００９８】

図８の説明に戻る。フラッシュメモリ６０４には、ピコネット内同期確立後に、通信相手のブルートゥースデバイスを認証したり、送信するデータを暗号化したりするためのリンクキーなどが記憶され、必要に応じてＣＰＵ６０１に提供される。

【００９９】

入出力インタフェース６０６は、ＣＰＵ６０１からの指示に基づく供給データ、およびベースバンド制御部６０７から供給されてきたデータの入出力を管理する。

【０１００】

ベースバンド制御部６０７は、トランシーバ６０８の制御、リンクの制御、パケットの制御、論理チャネルの制御、セキュリティの制御などの各種の制御、および誤り訂正符号化、復号化、或いはデータのランダム化などの処理を行い、入出力インタフェース６０６から供給されてきたデータをアナログ変換してトランシーバ６０８に出力するとともに、トランシーバ６０８から供給されてきた信号をデジタル変換して得られたデータを入出力インタフェース６０６に出力する。

【０１０１】

トランシーバ６０８は、ＧＦＳＫ(Gaussian Frequency Shift Keying)変調部、ＧＦＳＫ復調部、スペクトラム拡散部、逆スペクトラム拡散部、或いはホッピングシンセサイザ部等より構成され、ベースバンド制御部６０７から供給されてきた信号に各種の処理を施し、アンテナ６０９に出力するとともに、アンテナ６０９から供給されてきた信号に各種の処理を施し、得られた信号をベースバンド制御部６０７に出力する。

【０１０２】

トランシーバ６０８を構成するＧＦＳＫ変調部は、ベースバンド制御部６０７から供給されてきたデータの高域成分をフィルタにより制限し、１次変調として周波数変調を行い

、取得したデータをスペクトラム拡散部に出力する。スペクトラム拡散部は、上述したようにＬＡＰ全体の２４ビットとＵＡＰの下位４ビットからなる２８ビットにより算出され、ホッピングシンセサイザ部から通知される周波数ホッピングパターンに基づいて搬送周波数を切り替え、供給されてきたデータに対してスペクトラム拡散を施した後に得られた信号をアンテナ６０９に出力する。ブルートゥースにおいては、スペクトラム拡散部は、６２５μ秒毎に周波数をホッピングさせて、データを送信するようになされている。

【０１０３】

また、トランシーバ６０８を構成する逆スペクトラム拡散部は、ホッピングシンセサイザ部から通知される周波数ホッピングパターンに基づいて受信周波数をホッピングさせ、例えば、通信相手のスレーブから送信されてきた信号を取得する。また、逆スペクトラム拡散部は、取得した信号を逆スペクトラム拡散し、通信相手のスレーブからの信号を再生した後に得られた信号をＧＦＳＫ復調部に出力する。ＧＦＳＫ復調部は、逆スペクトラム拡散部から供給されてきた信号をＧＦＳＫ復調し、得られたデータをベースバンド制御部６０７に出力する。

【０１０４】

トランシーバ６０８は、２．４ＧＨｚ帯を使用して、スペクトラム拡散が施された信号をアンテナ６０９から送信する。また、トランシーバ６０８は、アンテナ６０９からの受信信号を逆スペクトラム拡散部に出力する。

【０１０５】

なお、ピコネットを構成する通信処理装置の各々は、図８に示したブルートゥースモジュール６００と同様の構成を有するモジュールを備えており、上述の処理により各装置各のデータ通信を実行する。

【０１０６】

上述したように、ブルートゥース規格に従った通信構成では、各機器はブルートゥースデバイス・アドレス（図９参照）という４８ビットのＩＤを持つことが定められている。そして、このＩＤはブルートゥース規格に従った通信において、通信相手を特定するのに使用される。

【０１０７】

通常、ブルートゥースデバイス・アドレスの情報は、図８を参照して説明したように、ブルートゥースモジュールのＩＣに直接つながる不揮発性メモリ（フラッシュメモリ６０４）に書き込まれており、ソフトウェアなどで読み出すことはできるが、変更することはできない。

【０１０８】

本実施例の認証シーケンスにおいては、ブルートゥースデバイス・アドレスを、２つの異なる方法で受信し、両者を比較して、一致すればローカル接続された機器間の通信、例えば同一のピコネットに接続された機器間の通信であると判定し、異なる場合には、外部ネットワークを介した通信であると判定する。

【０１０９】

ブルートゥースデバイス・アドレスの取得処理は、以下の２つの取得処理によって取得したアドレスの比較を行う。

（１）通信相手のブルートゥースデバイス・アドレスの情報をブルートゥース通信パケットのソースアドレスとして取得する。

（２）例えば、２つの機器が共有する秘密鍵をもとにブルートゥースデバイス・アドレスを暗号化して伝送するプロトコルを決め、このプロトコルに従ってブルートゥースデバイス・アドレスを取得する。

【０１１０】

このように、通信先デバイスの送信するパケットのソースアドレスとしてのブルートゥースデバイス・アドレスと、アプリケーションレベルにおけるデータ処理によってパケットに格納したブルートゥースデバイス・アドレスまたはブルートゥースデバイス・アドレスに基づく２つのブルートゥースデバイス・アドレスを取得し、これらの照合を実行する

。

【０１１１】

受信機器において、上記２つの方法で受信したブルートゥースデバイス・アドレスを比較して、一致すればローカル接続された機器間の通信、例えば同一のピコネットに接続された機器間の通信であると判定し、異なる場合には、外部ネットワークを介した通信であると判定する。

【０１１２】

ブルートゥース規格に従った通信を実行する機器同士で通信を行う場合、先に説明した図６（ｂ）のように、機器Ｘが機器Ｃに、また機器Ｙが機器Ａになりすますことでブルートゥース通信範囲を超えた通信を行うことも可能である。これを防ぐため、機器Ａは通信相手からきたパケットのソースアドレスとして入っているブルートゥースデバイス・アドレスと、前述の別のプロトコルによっても暗号などで保護されたブルートゥースデバイス・アドレスを取得する。

【０１１３】

この場合、ブルートゥースパケットのソースアドレスには機器Ｘのブルートゥースデバイス・アドレスが設定されており、機器Ａと秘密鍵を共有する機器は機器Ｃなので、機器Ｘ、Ｙ経由で機器Ｃのブルートゥースデバイス・アドレスを取得することになる。そして、これらのブルートゥースデバイス・アドレスの照合により、不一致が判明すると、機器Ｃがブルートゥースによるローカル通信領域、例えば同一のピコネットに存在しないと判定し、外部ネットワークに中継された通信を停止し、コンテンツ流出等の秘密情報の漏洩を防止することができる。

【０１１４】

上述したように、本発明の構成によれば、ホームネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となる。

【０１１５】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１１６】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１１７】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１１８】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインス

トールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０１１９】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【産業上の利用可能性】

【０１２０】

以上、説明したように、本発明の構成によれば、ホームネットワーク等のネットワークに対して、インターネット等の外部ネットワークに接続された機器からアクセスされた場合、そのアクセスが外部機器からか内部のローカルネットワーク内の機器からであるかを明確に判別することが可能となり、ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの漏洩、流出を未然に防止することが可能となり、コンテンツ著作権の管理の必要なコンテンツや、私的コンテンツ等、漏洩を防止することが必要なデータをローカルネットワーク内でのみ利用しようとするシステムにおいて適用されるデバイスで実行する認証シーケンスとしての適用が可能である。

【図面の簡単な説明】

【０１２１】

【図１】ネットワーク構成例について説明する図である。

【図２】通信処理装置の構成について説明する図である。

【図３】ＩＥＥＥ１３９４機器の構成について説明する図である。

【図４】本発明の認証シーケンスについて説明するフロー図である。

【図５】本発明の認証シーケンスについて説明するシーケンス図である。

【図６】本発明の認証シーケンスによるＩＤ取得処理および効果について説明する図である。

【図７】ブルートゥース規格による通信ネットワークについて説明する図である。

【図８】ブルートゥースデバイスの構成について説明する図である。

【図９】ブルートゥースデバイスの通信において適用されるブルートゥースデバイス・アドレスの構成について説明する図である。

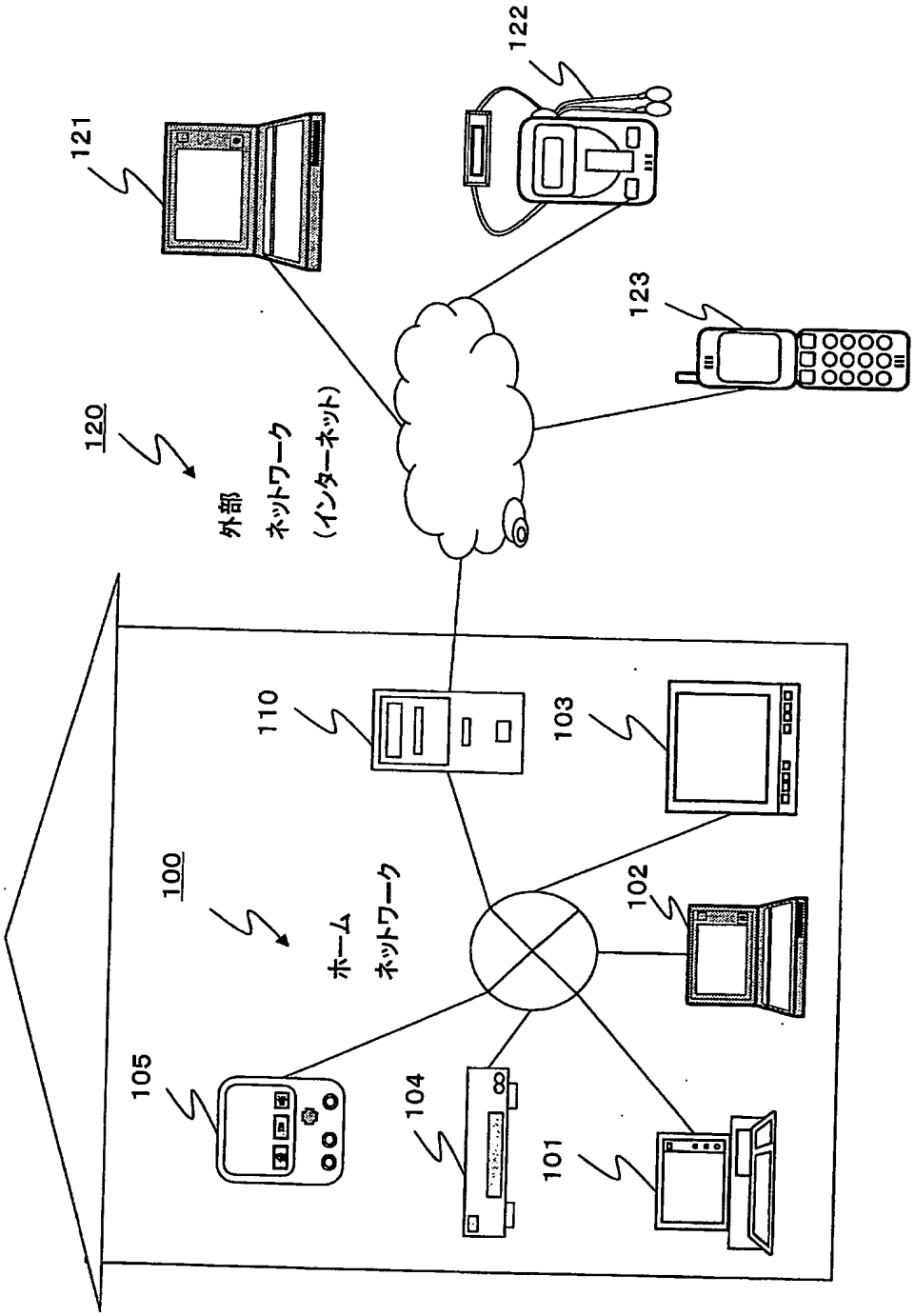
【符号の説明】

【０１２２】

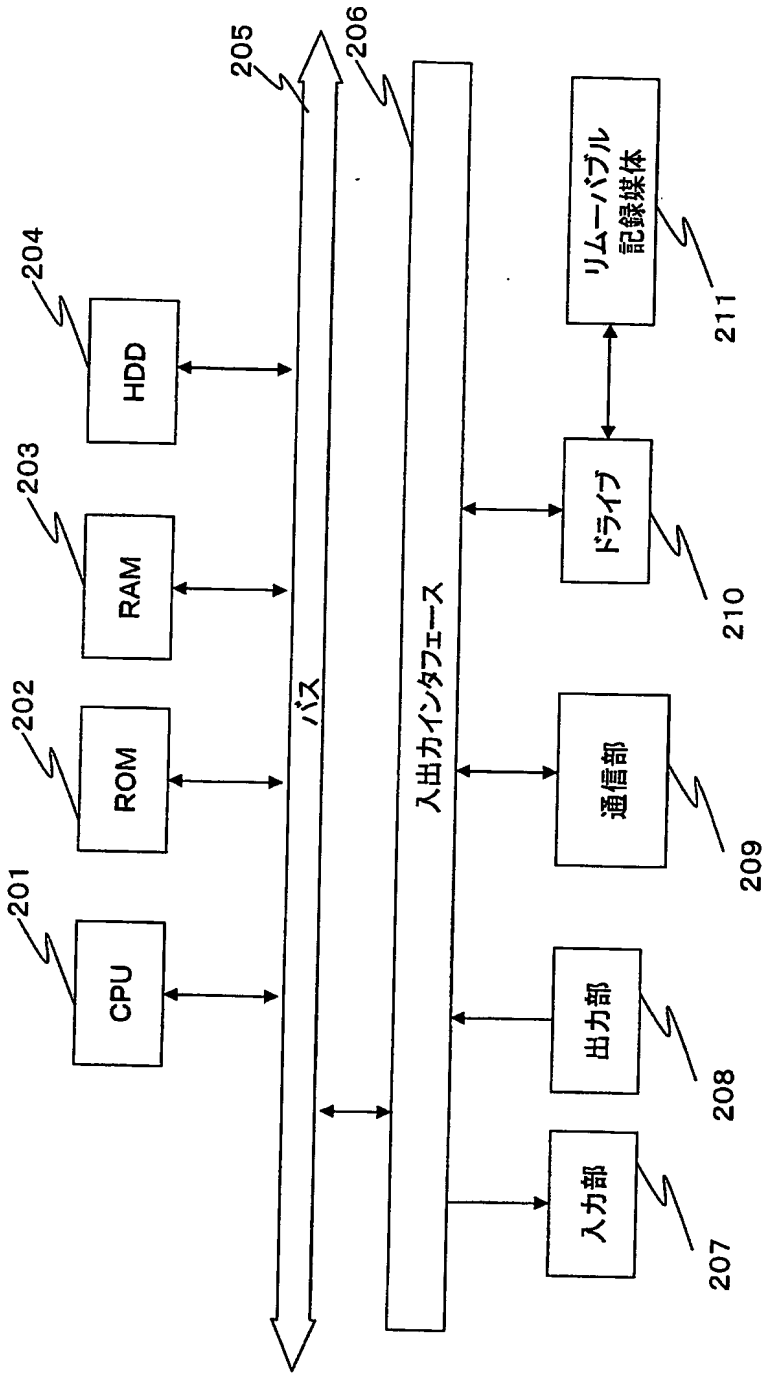
１００　ホームネットワーク
１０１　ＰＣ
１０２　ＰＣ
１０３　ＴＶ
１０４　ハードディスクレコーダ
１０５　ＰＤＡ
１２０　外部ネットワーク
１２１　ＰＣ
１２２　携帯電話
１２３　ポータブル再生プレーヤ
２０１　ＣＰＵ(Central Processing Unit)
２０２　ＲＯＭ(Read Only Memory)
２０３　ＲＡＭ(Random Access Memory)
２０４　ＨＤＤ(Hard Disk Drive)
２０５　バス
２０６　入出力インタフェース

２０７　入力部
２０８　出力部
２０９　通信部
２１０　ドライブ
２１１　リムーバブル記録媒体
３０１　送受信部
３０２　ＩＥＥＥ１３９４端子
３０３　ＰＨＹ－ＩＣ（ＰＨＹ通信部）
３０４　ＬＩＮＫ－ＩＣ
３０５　ネットワーク通信部（ＩＥＥＥ１３９４制御マイコン）
３０６　機器制御マイコン
３１０　１３９４バス
４１１　機器Ａ
４１２　機器Ｂ
４２１　機器Ａ
４２２　機器Ｃ
４３１　機器Ｘ
５０１　パーソナルコンピュータ（ＰＣ）
５２１　パーソナルコンピュータ（ＰＣ）
５２２　携帯電話
５２３　ＰＤＡ（Personal Digital Assistants）
５２４　ビデオカメラ
６００　ブルートゥースモジュール
６０１　ＣＰＵ
６０２　ＲＯＭ
６０３　ＲＡＭ
６０４　フラッシュメモリ
６０５　バス
６０６　入出力インタフェース
６０７　ベースバンド制御部
６０８　トランシーバ
６０９　アンテナ

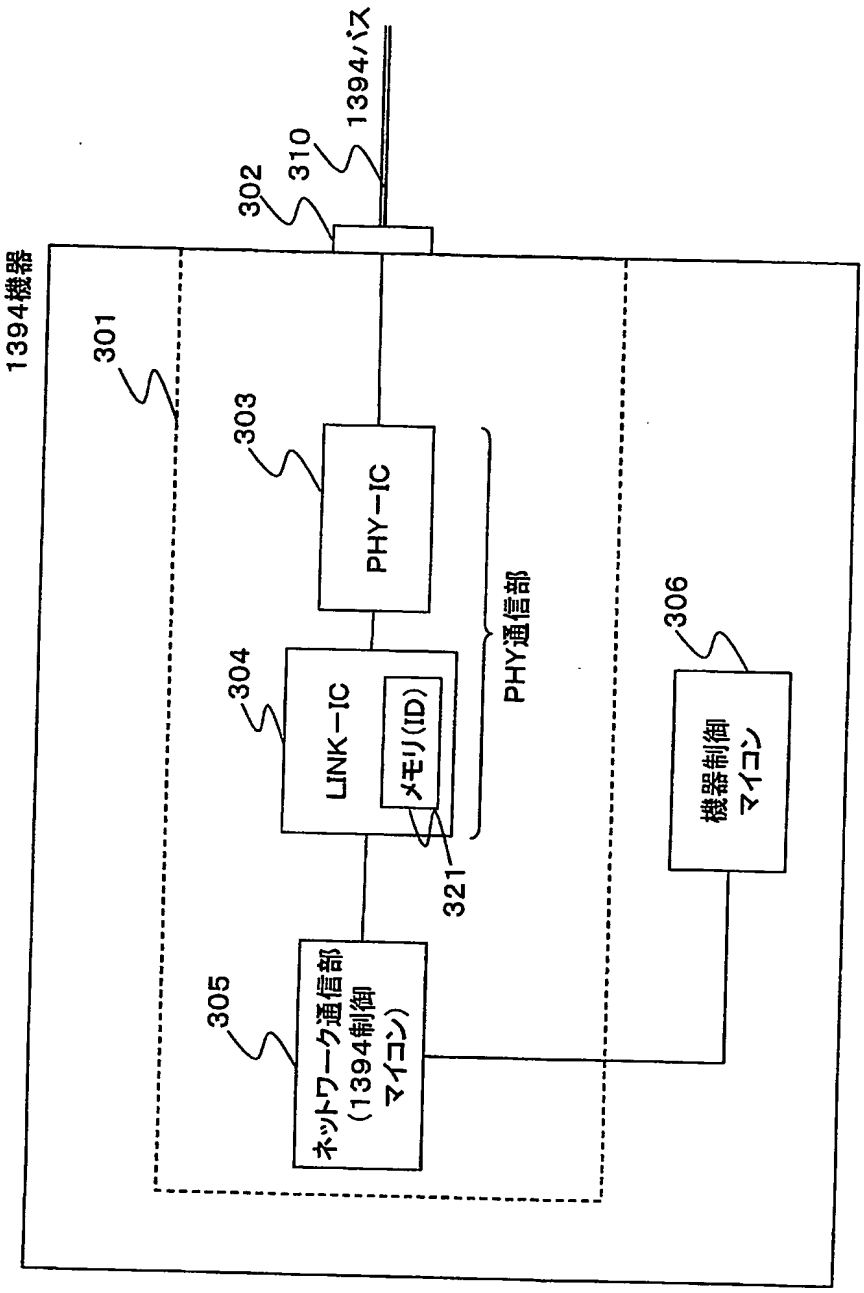
【書類名】図面
【図１】


122
121
123
120
外部
ネットワーク
（インターネット）
110
103
100
ホーム
ネットワーク
102
105
104
101

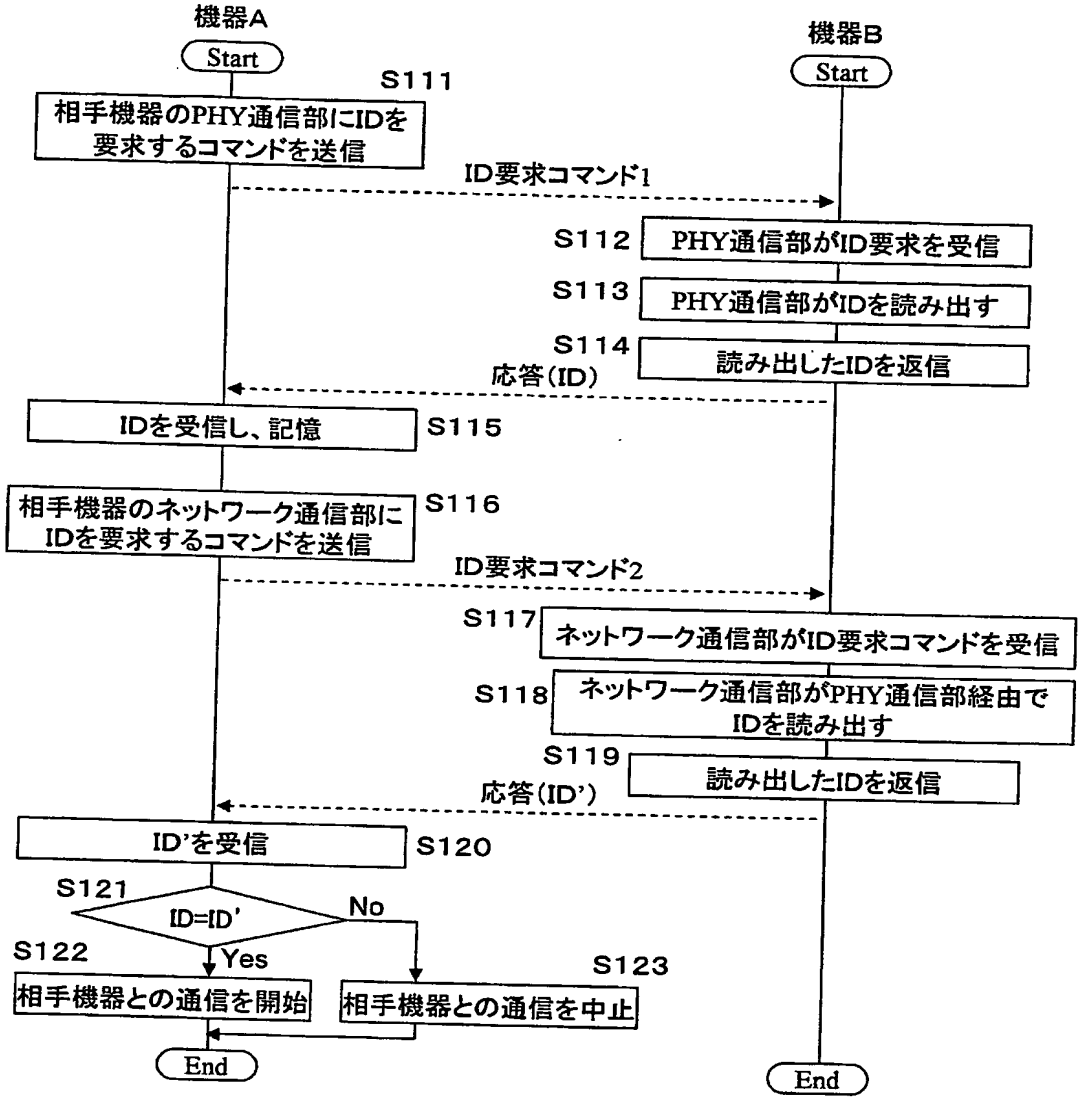
【図２】


205
206
204
HDD
203
RAM
202
ROM
201
CPU
バス
入出力インタフェース
リムーバブル記録媒体
211
ドライブ
210
通信部
209
出力部
208
入力部
207

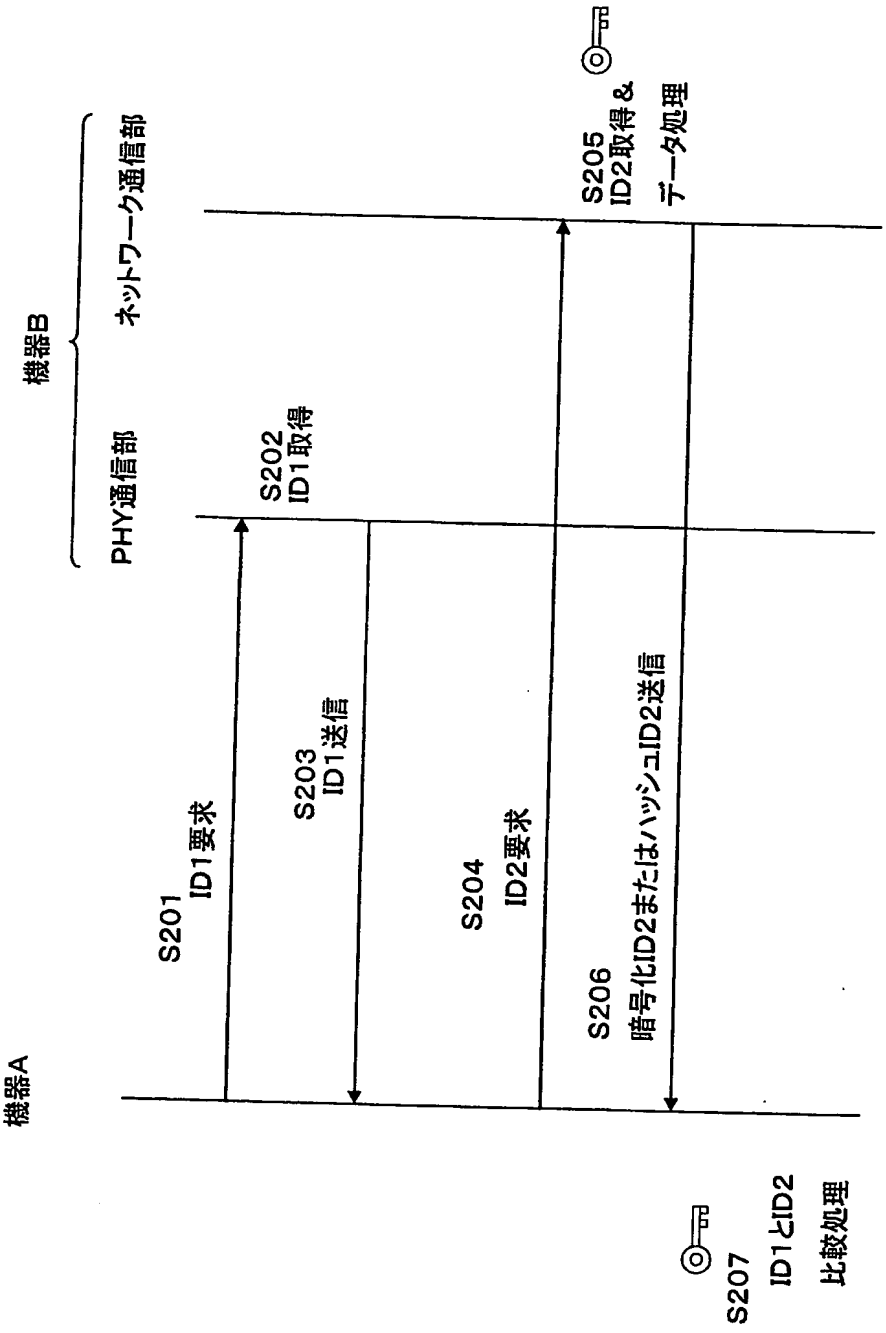
【図３】


1394バス
310
302
1394機器
301
303
PHY－IC
PHY通信部
306
304
LINK－IC
メモリ(ID)
機器制御
マイコン
321
305
ネットワーク通信部
(1394制御
マイコン)

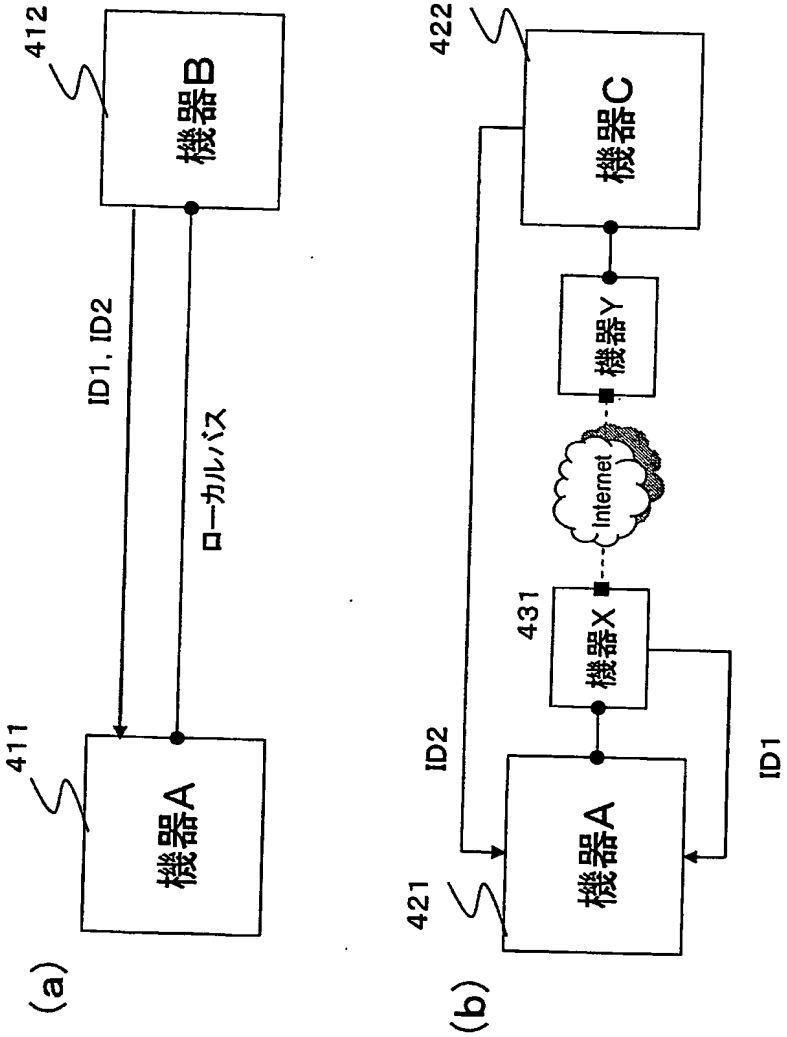
【図４】


機器A
Start
S111
相手機器のPHY通信部にIDを要求するコマンドを送信
ID要求コマンド1
機器B
Start
S112
PHY通信部がID要求を受信
S113
PHY通信部がIDを読み出す
S114
読み出したIDを返信
応答(ID)
IDを受信し、記憶
S115
相手機器のネットワーク通信部にIDを要求するコマンドを送信
S116
ID要求コマンド2
S117
ネットワーク通信部がID要求コマンドを受信
S118
ネットワーク通信部がPHY通信部経由でIDを読み出す
S119
読み出したIDを返信
応答(ID')
ID'を受信
S120
S121
ID=ID'
No
Yes
S122
相手機器との通信を開始
S123
相手機器との通信を中止
End
End

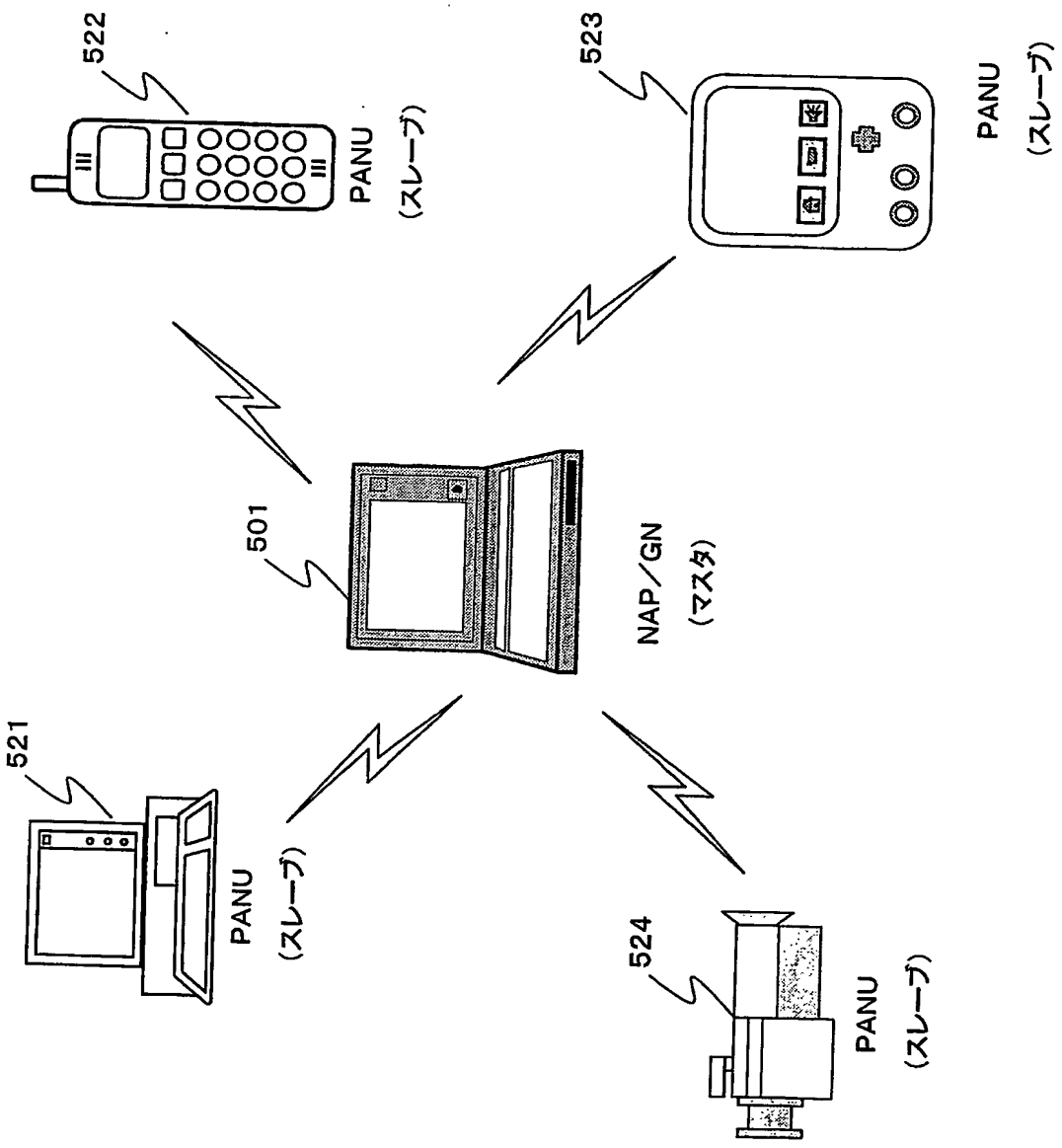
【図５】


機器B
ネットワーク通信部
PHY通信部
機器A
S201
ID1要求
S202
ID1取得
S203
ID1送信
S204
ID2要求
S205
ID2取得＆
データ処理
S206
暗号化ID2またはハッシュID2送信
S207
ID1とID2
比較処理

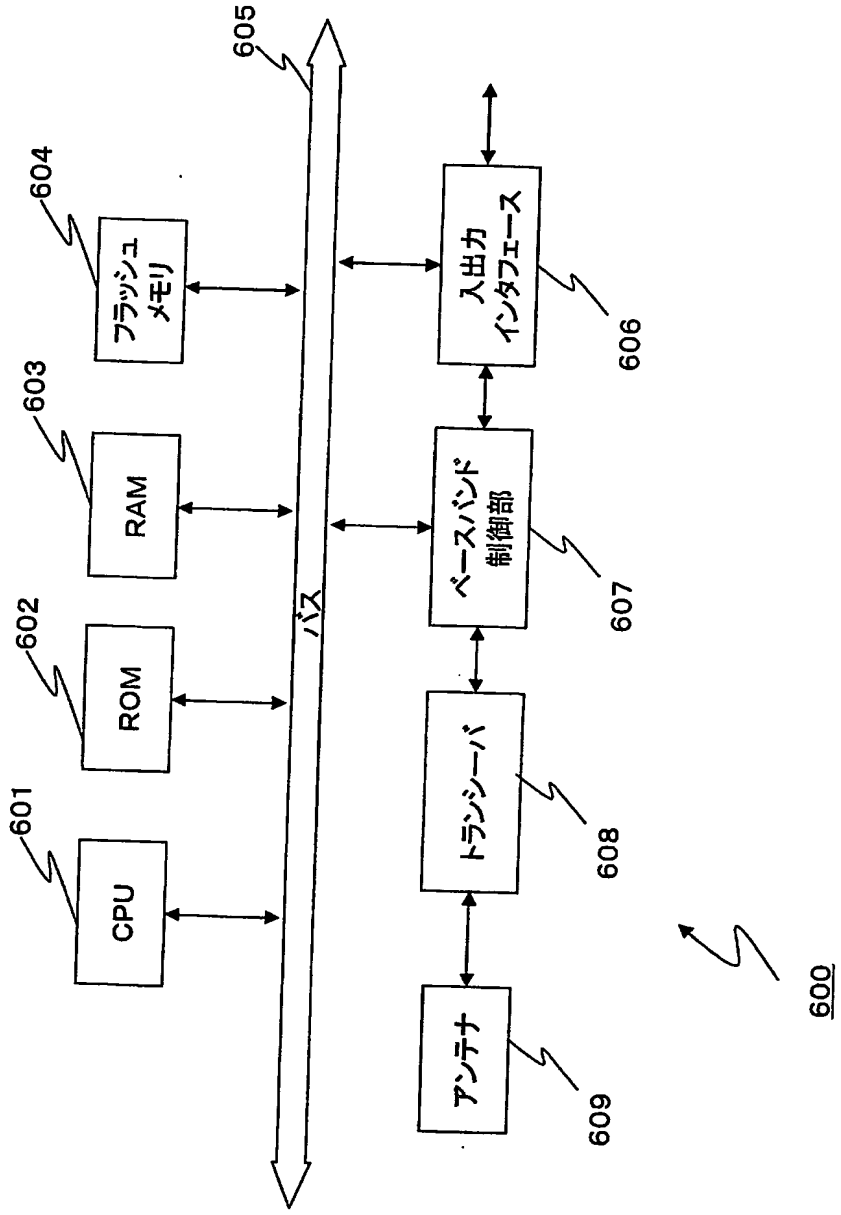
【図６】


412
機器B
ID1, ID2
ローカルバス
411
機器A
(a)
422
機器C
機器Y
Internet
431
機器X
ID2
ID1
421
機器A
(b)

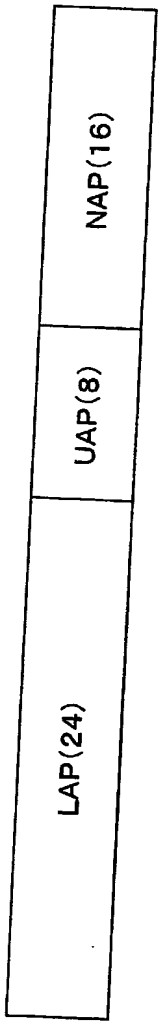
【図７】


522
PANU
(スレーブ)
523
PANU
(スレーブ)
501
NAP／GN
(マスタ)
521
PANU
(スレーブ)
524
PANU
(スレーブ)

【図８】


605
604
フラッシュメモリ
603
RAM
602
ROM
601
CPU
バス
入出力インタフェース
606
ベースバンド制御部
607
トランシーバ
608
アンテナ
609
600

【図９】



【書類名】要約書
【要約】
【課題】　ローカルネットワーク内の秘密情報、例えば私的データや、著作権、利用権の制限されたコンテンツの外部に対する漏洩、流出を未然に防止することを可能とした構成を提供する。
【解決手段】　通信先デバイスの識別情報を異なるデータ処理レベルで複数取得する。例えばＯＳＩ参照モデルにおける物理層またはデータリンク層レベルにおけるデータ処理によって取得した識別情報と、ネットワーク層以上の層レベルにおけるデータ処理によって取得した識別情報とを受信し、これらの識別情報の照合を行う。また、少なくとも１つの識別情報は、通信元デバイスと共有する秘密情報に基づく暗号処理またはハッシュ値生成による生成データを受信する。複数の識別情報の照合を行い、照合の成立または非成立に基づいて、通信先デバイスが同一のローカルネットワークに接続されたデバイスであるか否かを判定する。
【選択図】　図５

特願２００３－２９１９７１

出　願　人　履　歴　情　報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社